

**Testimony of**  
**Jonathan Gold**  
**Vice President, Global Supply Chain Policy**  
**The Retail Industry Leaders Association**  
**Submitted for the**  
**House Committee on Homeland Security**  
**Hearing on**  
**Security and Accountability For Every (SAFE) Port Act**  
**April 4, 2006**

Good morning. Chairman King, Ranking member Thompson and other distinguished members of the committee. My name is Jonathan Gold and on behalf of the Retail Industry Leaders Association (RILA), I thank you for the opportunity to testify at this important hearing regarding the Security and Accountability For Every (SAFE) Port Act.

By way of background, the Retail Industry Leaders Association (RILA) is a trade association of the largest and fastest growing companies in the retail industry. Its member companies include more than 400 retailers, product manufacturers, and service suppliers, which together account for more than \$1.4 trillion in annual sales. RILA members operate more than 100,000 stores, manufacturing facilities and distribution centers, have facilities in all 50 states, and provide millions of jobs domestically and worldwide.

I also serve as a member of the Department of Homeland Security's Advisory Committee on the Commercial Operations of Customs and Border Protection (COAC). Prior to serving on the COAC I participated in several of the subcommittees as a technical advisor, including the subcommittee working on implementation of the 24-Hour rule, implementation of the Maritime Transportation Security Act and the Customs-Trade Partnership Against Terrorism (C-TPAT) subcommittee, which helped to update the importer criteria last year.

RILA members share this Committee's, and indeed all Americans, common goal of making the global supply chain and the movement of cargo through the global supply chain as safe and secure as possible. As the largest users in the global maritime supply chain, we have an enormous stake in cargo security and are committed to helping the government further enhance security throughout the system. While a great deal has been accomplished to improve supply chain security since the tragic events of September 11, 2001, the government and private sector stakeholders must continue to work together to improve security. RILA commends the members of this Committee for striving to identify and address the vulnerabilities in our maritime supply chain system.

We strongly believe that security legislation, regulations, and public-private partnerships can achieve the dual objectives of enhancing security while continuing to facilitate legitimate global commerce. We urge Congress to avoid measures that have a very limited effect on enhancing security while actually impeding the flow of legitimate commerce and creating a false sense of security. A primary goal of those who would disrupt the supply chain is to damage the U.S. economy by any means possible. If commerce is disrupted in a way that damages the ability of Americans to hold well-paying jobs, provide for their families, and generate economic growth that helps the entire world, either through an attack or ill-conceived regulation of our international trading system, then the terrorists will have achieved one of their key goals.

Supply chain security is a global issue that cannot be addressed unilaterally. The most effective supply chain security measures are those that push our borders out, assessing vulnerabilities and identifying threats to cargo shipments before they reach U.S. ports. Effective cargo security requires a multi-layered, unified approach that must be international in scope. While recent policy debates have focused on who owns assets in the supply chain system, nobody should dispute that it is better to detect or disarm weapons or contraband thousands of miles from our shores than after their arrival in the U.S.

RILA and its members have played a critical leadership role in shaping supply chain security efforts. From requiring new security language in contracts with their business partners to testing new technologies and ways to identify container tampering, private sector stakeholders have been the innovators in securing their supply chains to protect their employees, customers

and businesses. In considering the SAFE Ports Act, we urge Congress to continue to allow the private sector, working closely with the Department of Homeland Security and other government and non-government interests, to test and deploy the systems and technologies that prove most effective. No one has a greater interest in security than the private sector companies who depend on a secure and efficient supply chain for the safety of their employees and customers and efficient operations of their businesses.

As members of the Committee are aware, a number of regulations and initiatives have already been undertaken to protect the U.S. from a terrorist attack affecting the supply chain. RILA members have supported a number of these initiatives, such as the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the 24-Hour Rule, the Bioterrorism Act, the Maritime Transportation Security Act (MTSA) and the International Ship and Port Facility Security Code (ISPS). Targeting different aspects of supply chain security, these regulations and initiatives together represent a strong foundation upon which the SAFE Ports Act and other initiatives must build to enhance our nation's maritime supply chain security.

On March 9, RILA wrote a letter to every member of Congress suggesting some key areas where both Congress and the Department should focus on to improve cargo security. These include:

- Improve the Automated Targeting System to ensure Customs and Border Protection (CBP) has the right information to determine whether or not a container poses a risk.
- Ensure CBP has sufficient resources to conduct C-TPAT validations.
- Work with CBP to improve CSI to conduct more cargo screening abroad, with a special emphasis on the quality of screening for nuclear and radiological material.
- Ensure that all aspects of MTSA are implemented, including the Transportation Worker Identification Credential (TWIC).
- Further develop business continuation and restoration of trade plans.

In most respects, the SAFE Ports Act is well aligned with these recommendations. For purposes of this written testimony, I would like to discuss some of the key sections of the bill and share RILA's perspective:

#### **Section 4- Strategic Plan**

RILA strongly supports the development of a strategic plan for cargo security. We believe that an initial version of this plan already exists under the National Strategy on Maritime Security. Further efforts should seek to improve this plan and its eight supporting plans, in particular the Maritime Incident Response Plan.

#### **Section 5 Protocols for the Resumption of Trade**

RILA members commend the Committee for including consideration of mechanisms to provide for continuity planning and restoration of trade in the event of a maritime security incident. The United States is in dire need of a well-coordinated response plan among all levels of government to ensure that commerce continues to move throughout the supply chain should

an incident occur. In addition, Congress and the Administration need to ensure that the various agencies involved in homeland security do not duplicate ongoing efforts. In short, the government, the business community and key stakeholders throughout the international trading system must be on the same page and know there is a plan in place to respond to an incident of national significance occurring as a result of terrorism or national disaster.

For example, if an incident were to occur in the Port of Los Angeles, that port, as well as the Port of Long Beach, might have to be shut down during the incident investigation and response. What would happen to other ports on the West Coast? Would Seattle/Tacoma remain open? Would incoming cargo be able to be diverted to other ports? While individual ports have worked on contingency plans for their own facilities, have there been discussions among ports geographically located near each other as to how they would work together? Will all maritime vessels be required to stop where they are or will vessels at non-incident ports be allowed to continue to move?

It is not clear to the business community at this time as to who will be making these critical decisions. The trade community needs this vital information to plan appropriately. While security concerns may require that certain details need to be kept within the government sphere, RILA believes that a central communication point or channel must be established so that communications can be streamlined. DHS has begun to work on this issue with the release of the Maritime Incident Response Plan, but more work needs to be done. One needs only to look at the experience of Hurricane Katrina to understand the need to have a well-coordinated response that ensures commerce will continue to flow through our nations' ports in the wake of an incident.

Likewise, each country has an interest in ensuring that the global supply chain is kept safe. A major terrorist incident in the U.S. will not impact just one port or one city or even one country. The impact will be felt around the globe. Careful planning and cooperation among governments is important, and government's active collaboration with the private sector is extremely critical. Supply chain security is simply too complicated for the public sector to act effectively without partnering with private industry.

## **Section 6 - Enhanced High-Risk Targeting Capabilities**

CBP receives detailed information about every single container coming into the U.S. prior to that container being loaded at a foreign port, and has developed elaborate mechanisms to utilize intelligence and other risk factors to differentiate the true "needle in the haystack" from the overwhelming percentage of cargo containers that present no security risk. Again, setting arbitrary and mandatory percentages of cargo that must be physically inspected will do nothing to enhance security and would be contrary to the mission of the effective risk management system DHS already has in place.

Better identification of high-risk cargo represents the best use of government resources and should be the goal of this and any legislation addressing cargo container security. RILA is committed to improving cargo container screening by identifying additional cargo data that can help with the identification of high-risk cargo. DHS should work with cargo owners and others who own supply chain information to determine what data elements are needed for security risk assessment, who has the information, when the information can be submitted, how it will be used and, most importantly, how it will be protected.

## **Section 8 - Verification of Individuals with Access to Secure Areas of Seaports**

In keeping with increasing security at U.S. ports, RILA also endorses prompt implementation of the Transportation Workers Identification Credential (TWIC), a standardized ID containing biometric information that vets the identity and background of the cardholder. All individuals with access to cargo and secure areas of our nation's ports would carry the TWIC, and its potential for use extends to workers throughout our nation's critical infrastructure systems. We believe that verification of individuals with access to secure areas of critical infrastructure and identification of individuals with prior criminal records or indications of connections with terrorist elements are crucial steps toward strengthening security.

## **Section 10 - Container Security Standards and Verification**

Security must be built into the global supply chain from origin to delivery, leveraging the best of current and emerging technologies. Yet the recent GAO report also underscores the need to keep in mind that technology is only one part of the overall solution. Put simply, there is no technological "silver bullet" for supply chain security. We must be wary of adopting technological solutions that merely create a false sense of security. Too much is at stake to put our trust behind cosmetic, "feel good" security measures.

RILA encourages appropriate testing of all proposed technology solutions to determine which have the greatest reliability before being adopted by the government and industry. It is important that promising technologies be developed by dedicating adequate funds for research and development. At the same time, rushing unproven and/or faulty technology into supply chain security without thorough implementation testing solely for the sake of doing something about security will undermine progress made to date, contribute to a false sense of security and in the end, prove both costly and ineffective. The fact that a certain physical device or screening process may work well in a lab or at a particular port does not mean that it can or should be expanded to other real-world applications. Congress should outline policies and goals and let DHS find the smartest and most effective way to meet those goals rather than being forced into deploying unproven "gadgets." Before any technology can be mandated, DHS must ensure the technology's functionality and application as well as work with the trade community to determine the most effective methods to deploy them in order to achieve maximum results.

## **Section 11 - Nuclear and Radiological Detection Systems**

As DHS works to improve its supply chain security capabilities, RILA supports efforts to ensure that we have a "zero tolerance" policy for nuclear and radiological material entering our country. While it is preferable to have that screening done overseas as occurs at CSI ports covering the great majority of cargo bound for the U.S., so long as we allow smaller ports to ship to the U.S., we will need a robust detection regime at our domestic ports as well. Thus it should be the highest priority for CBP and DHS to ensure that those ports participating in the Container Security Initiative have the most effective technology available to detect radiation and that domestic ports achieve universal nuclear and radiological detection capability. Recent Government Accountability Office reports have identified weaknesses in both aspects of the nuclear and radiological detection regime, and RILA supports the work of the Domestic Nuclear Detection Office to build this most critical layer of our defenses.

In addition to the deployment of the Radiation Portal Monitors at U.S. ports, RILA also encourages DHS and CBP to consider other models to help conduct container screening overseas. One such model, which has received a great deal of attention, is the Integrated Container Inspection System (ICIS), which is currently being tested at two terminals in Hong Kong. While we, along with CBP, believe that this model fits with the multi-layered approach, there are still many questions and operational issues that need to be discussed and resolved before such a system is implemented on a global scale. We strongly urge DHS and CBP to continue to work with the private sector on ICIS and other models to successfully address the operational issues.

### **Section 13 – Customs-Trade Partnership Against Terrorism**

One cornerstone of the public-private, collaborative approach to supply chain security supported by RILA is the C-TPAT program, which reflects CBP's recognition that it can best provide security through close cooperation with the very businesses whose ability to recognize potential vulnerabilities in the supply chain is matched only by their desire to ensure that the system as a whole -- and each component part -- is as robust and secure as possible. The key to C-TPAT's success is the program's acknowledgement that there is no "one size fits all" approach to supply chain security, for individual C-TPAT member's supply chain functions, needs and vulnerabilities are not the same. What works for one industry, such as retail, may not be well suited for another industry, such as chemical.

While there has been some consideration given to placing C-TPAT under a strict regulatory regime, RILA members strongly believe that regulating this program will limit the very flexibility that is one of the program's greatest assets, and in turn harm the ability of government and industry to respond and adapt quickly to innovations and other changes related to the security dynamics of their specific link in the supply chain. Requiring changes to C-TPAT to go through a full regulatory rule-making process would be much slower and less nimble for CBP to turn current intelligence or perceived weaknesses into new security requirements.

In addition, the public-private partnership concept at the heart of C-TPAT's effectiveness would be compromised by the introduction of required "third party validators" acting as middlemen between government and the business community, adding a potentially cumbersome extra layer of communication to a direct, two-party dialogue. With a third party attempting to interpret and relay information from business to government, the potential for diminishing and delaying the quality of information exchanged is clear.

C-TPAT works because it provides incentives to participants to engage in active compliance with government security objectives by, for example, providing ATS scoring benefits to companies that meet the basic requirements of the program. RILA believes that continuing effective operation of the program depends on its ability to offer such baseline incentives for participation.

In addition, while we agree with the tiered approach as outlined by the bill and which CBP is currently using, we have concerns with Congress specifying what criteria companies must meet to achieve Tier Three status, especially the inclusion of language on container security devices. We do not believe Congress should mandate such devices as they are still being tested and are not yet at 100% overall reliability and still have many operations questions that need to be answered.

## **“Sail Only if Scanned Act of 2006” Comments**

While the focus of this hearing is on the SAFE Ports Act, I would be remiss in not making some comments about the “Sail Only if Scanned Act of 2006,” which was offered as an amendment during last week’s markup.

RILA supports 100% *screening* of high risk containers, but a policy requiring 100% scanning of all U.S. bound containers is neither effective as a deterrent nor feasible operationally as a security enhancement measure. Rather than enhancing security, setting an arbitrary number of scanning or inspections of containers would result in commerce grinding to a halt, in effect creating much of the same harm to the nations and the world’s economy that a terrorist incident would cause.

The legislation as drafted is very vague and confusing. While the bill calls for “scanning” of all containers for radiation and density, this term is not specifically defined. Is this a scan for radiological material? Is it a scan using a non-intrusive X-ray? These are two very different technologies that have different requirements and have different impacts on the movement of legitimate cargo.

There are also many questions about who would be conducting the scanning when the scanning would occur, to whom the scanned images would be sent and what would be done with the images. There is also a question whether the U.S. can mandate such a requirement on foreign terminal operators and foreign governments, which is why CBP has negotiated cooperative agreements, such as the Container Security Initiative, with foreign countries to allow screening on their soil. In addition, if we ask our foreign trading partners to put such a requirement in place, we must be prepared to do the same here in the U.S. as calls for reciprocity will surely be made.

In addition, the bill includes requirements for a container seal that can detect and track whether a container has been tampered with after loading. As discussed above, technology to accomplish this goal is still being tested in the harsh real-world environment in which international cargo must exist.

## **Conclusion**

I would like to thank the House Committee on Homeland Security for the opportunity to testify today. RILA applauds the initiative of the Committee to further enhance supply chain security and congratulates Chairman King, Chairman Lungren, Ranking Members Thompson and Sanchez and Congresswoman Harman and their staffs for focusing attention on these key issues. RILA strongly believes that government, industry and other stakeholders need to maintain an ongoing, robust dialogue on how best to strengthen port and supply chain security, rather than allowing the debate to intensify and recede as dictated by external factors.

RILA and its members stand ready to continue to work with both Congress and the Administration on improving the security of U.S. ports and the global supply chain. I look forward to taking your questions.